Cisco Trust Anchor Technologies

Overview

Cisco® Trust Anchor Technologies provide the foundation for trustworthy systems across Cisco. The Cisco Trust Anchor and a Secure Boot check of signed images help ensure that the code running on Cisco hardware platforms is authentic and unmodified, establishing a hardware-level root of trust and an immutable device identity for the system to build on.

Validation of all levels of software running on the platform during startup establishes a chain of trust for the system. Validation of boot code integrity is mandated in the Cisco Secure Development Lifecycle for all Cisco platform-based products.

Cisco Trust Anchor Technologies provide product assurance functionality as well as foundational security features: immutable identity, highly secure storage, a random bit generator, and secure key management.

Why Should You Choose Cisco?

Cisco Trust Anchor Technologies start with standards-based technology and add security functions and features, providing cost-effective and efficient solutions for the protected product. Cisco's Secure Boot implementation not only provides a secure boot of signed images, but also anchors a root of trust into hardware components. The hardware components that start the chain of trust can perform both system-critical functions and security functions, including proactive monitoring of the startup process and a shutdown of the process if tampering is detected.

Why Cisco Trust Anchor Technologies Matter?

In today’s era of the Internet of Everything, security breaches are on the rise. Concerns of malicious attacks on hardware and software as well as full counterfeiting of PCs, set-top boxes, servers, and other edge platforms in networking devices, ignited Cisco to proactively add Secure Boot, secure unique device identity and other Trust Anchor Technologies into our products.

Common questions based on these threats include:

- How do I know I am running Cisco’s genuine software and hardware?
- How do I know my software has not been modified before or during boot up?

Cisco Trust Anchor Technologies give customers the confidence that the product is genuine. The Cisco Secure Boot protects the boot code in the hardware and shows the image hashes as well as providing the secure unique device identification (SUDI).

How do you know that your device has implemented Cisco Trust Anchor Technologies?

The number of Cisco products that have implemented Cisco Trust Anchor Technologies is growing. Please contact your account manager or sales engineer for your device’s security profile.

What’s the risk of not implementing Cisco Trust Anchor Technologies?

The lack of a hardware-level root of trust has resulted in known hacks. Third parties can tamper with BIOS/ROM monitor (ROMMON) boot code to load modified software images; bypass hardware, authenticity, and licensing checks; or perform additional functions with malicious intent. Tampered code can also result in data manipulation, data theft, the creation of a platform to launch attacks, and denial of service (DoS). Cisco Trust Anchor Technologies help close these potential security gaps.

Cisco Trust Anchor Technologies also enhance our supply chain security. Cisco mandates supply chain and development security across its product lifecycle with a focus on process, policy, and technology.

Fundamental Concepts of Cisco Trust Anchor Technologies

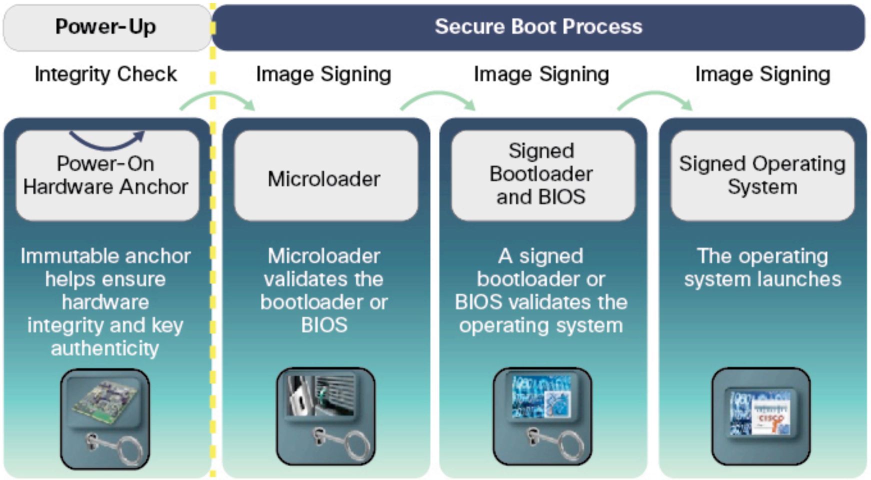
Image Signing and Trust Chains

- **Digital signing:** Digital signing (often called code or image signing) involves creating a unique digital signature for a given block of data such as software code. The signature is created with a hashing algorithm, similar to a checksum, to compute a “hash value” for the code. This hash value is then encrypted using a signing key. Signed code is checked at runtime to verify that it has not been changed. Typically the code gets a signature calculated by the code owner, and this signature is stored on the system along with the code. Before the signed code is run, it can be validated by a trusted system element using the same algorithm to create its own signature, which is then compared with the precomputed stored signature. Signing can be subverted if code-protection measures are not in place to prevent changes in the code or system that bypass signing checks.
- **Trusted element:** A trusted element in the scope of system software is a piece of code that is known to be authentic. Code that cannot be changed at all is often called immutable (that is, unable to be changed). A trusted element is either immutable (stored in such a way as to prevent modification) or authenticated through validation mechanisms.

- **Root of trust:** The root of trust is the anchor for the system at which a guaranteed trusted element exists. If the first code running on a system is immutable, it becomes the root of trust in that system.
- **Chain of trust:** A chain of trust exists when the integrity of each element of code on a system is validated before that piece of code is allowed to run. A chain of trust starts with a root of trust element. The root of trust validates the next element in the chain (usually firmware) before it is allowed to start, and so on.

Through the use of signing and trusted elements, a chain of trust can be created for the software running on Cisco platforms throughout the network. Cisco Trust Anchor Technologies are used to establish the root of trust in that trusted chain. (See Figure 1.)

Figure 1. Image Signing and Trust Chains



Power-Up
Secure Boot Process
Integrity Check
Image Signing
Image Signing
Image Signing
Power-On Hardware Anchor
Microloader
Signed Bootloader and BIOS
Signed Operating System
Immutable anchor helps ensure hardware integrity and key authenticity
Microloader validates the bootloader or BIOS
A signed bootloader or BIOS validates the operating system
The operating system launches

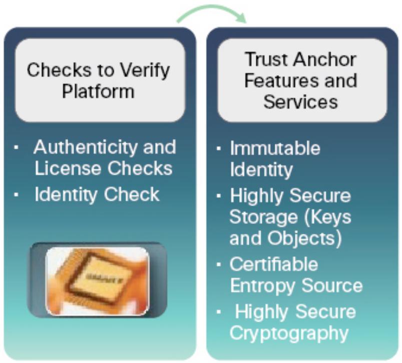
Immutable Identity—SUDI

The SUDI is an X.509v3 certificate, which maintains the product identifier and serial number. The identity is implemented at manufacturing and chained to a publicly identifiable root certificate authority. It can be used as an unchangeable identity for configuration, security, auditing, and management.

The SUDI credential in the Trust Anchor can be either RSA or Elliptic Curve Digital Signature Algorithm (ECDSA) based. The SUDI certificate, the associated key pair, and its entire certificate chain are stored in the tamper-resistant Trust Anchor chip. Furthermore, the key pair is cryptographically bound to a specific Trust Anchor chip and the private key is never exported. This feature makes cloning or spoofing the identity information virtually impossible.

The SUDI can be used for asymmetric key operations such as encryption, decryption, signing, and verifying that allow passage of the data to be operated upon. This capability makes remote verification of a device’s authentication possible. It enables accurate, consistent, and electronic identification of Cisco products for asset management, version visibility, service entitlement, quality feedback, and inventory management. (See Figure 2.)

Figure 2. Immutable Identity—SUDI


Checks to Verify Platform
• Authenticity and License Checks
• Identity Check
Trust Anchor Features and Services
• Immutable Identity
• Highly Secure Storage (Keys and Objects)
• Certifiable Entropy Source
• Highly Secure Cryptography

Highly Secure Storage

Cisco Trust Anchor provides highly secure storage for keys, passwords, customer credentials, and other critical security information for the device. One of its advantages is the ability to store private encryption keys and passwords for even greater security. Storage secured outside using the Trust Anchor encryption is also possible.

Random Number Generation and Entropy Source

Strong random number generation (RNG) is at the core of encryption, and weak RNG can undo the entire encryption system. Random number generators play a key role in creating cryptographic keys, in opening highly secure communications between users and websites, and in resetting passwords for email accounts. Without assured randomness, an attacker can predict what the system will generate and undermine the algorithm.

The Cisco Trust Anchor is compliant with NIST specifications and provides a NIST SP 800-90A and B certifiable RNG that extracts entropy from a true random source within the Trust Anchor.

Data-at-Rest Encryption and Decryption Functions Using Secure Keys

The Cisco Trust Anchor can also generate key pairs that can be used for customer-controlled certificates commonly called locally significant certificates (LSCs) or local device identity (LDevID) certificates.

Customer identity functions supported by the Trust Anchor include:

- Retrieval of LDevID RSA public keys
- Authentication with a certification authority (CA) before LSC enrollment
- Zero-touch provisioning authentication
- Secure Boot posture assessment

For More Information

For additional information about Cisco Trust Anchor Technologies, visit Cisco Trustworthy Systems: Secure Boot and Trust Anchor Solutions or write to ask-trustworthy@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C45-734230-00 03/15